Anno 6 – N.141
20 Dicembre 2007/ 09 Gennaio 2008

Editore (sede legale):
WLF Publishing S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

Allarmismo col trucco

"Anche nelle forze più socializzanti, troverete sempre qualche moto sotterraneo che tende a conquistare ed a mantenere il potere attraverso l'uso delle parole."
Frank Herbert

Si stanno ormai rincorrendo da un po' voci di un futuro collasso della rete globale previsto per il 2010... Ben due anni prima della fine del mondo secondo il calendario Maya... Per cortesia!!! Non prendeteci per degli stupidi, tutti sappiamo che l'aumento del traffico, la ricerca parla dei 27 Petabyte mensili (27.000.000 di gigabyte) usati di YouTube, sta deteriorando la rete ma questo non vuol certo dire che torneremo a navigare col modem dial up e che internet è destinato a morire... Per il gusto della polemica oltretutto ci è piaciuto andare a vedere chi erano i finanziatori della ricerca a cui fanno riferimento queste voci, quella pubblicata su USA Today, e abbiamo scoperto che si tratta, tra gli altri, di Internt Innovation Alliance, azienda di proprietà di At&t... Insomma sembra che il tutto sia stato un po' "pilotato" per convincere qualcuno, leggi i governi e le istituzioni, ha stanziare soldi, e molti, per il rinnovamento delle reti in modo da assicurarsi una pensione di tranquillità... Certo che noi siamo dalla parte del rinnovamento, siamo per avere sempre reti nuove e più veloci, soprattutto qua in Italia dove utilizziamo centrali di smistamento Telecom che saltano ogni 10 giorni e dove tutta la rete è ormai ben più che vecchia. Quello che ci disturba è che, come al solito, per portare avanti gli interessi di gruppi di potere si cerchi di mobilitare la gente attraverso falsi allarmismi che si basano fondamentalmente sull'ignoranza della gente riguardo argomenti come gli aspetti tecnici della rete. Insomma è ora di smetterla di muovere l'opinione pubblica a seconda degli interessi che si vogliono proteggere. Ma poi, volendo ben vedere, se avessero ragione i Maya, due anni senza rete possiamo anche farli...

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Come volevasi dimostrare...

:: Ne abbiamo parlato sull'ultimo numero...

"La polizia, la stessa che non è stata in grado di aprire i miei file criptati, è obbligata dalla legge a custodire i miei dati una volta che io gli abbia fornito la password, ma cosa mi garantisce che sia in grado di conservarli in maniera sicura in modo da salvaguardare la mia privacy???"
(Da Hacker Journal 140 - pagina 21)

E come volevasi dimostrare, pochi giorni dopo è successo il delirio, il governo di sua maestà è riuscito a perdere in un solo botto i dati personali di circa 25.000.000 di persone. I dati comprendevano tutto quanto di più privato e sensibile può esserci: date di nascita, recapiti, numeri di previdenza sociale e sanitaria e soprattutto i riferimenti dei conti bancari dove i malcapitati si facevano accreditare gli assegni familiari.
Ma come può capitare tutto ciò, come può succedere, qualche pirata informatico, un virus, un server che esplode, un palazzo che brucia... No!!! Nulla di tutto questo!!! Semplicemente hanno spedito due CD da un ufficio in provincia, il HM Revenue & Customs, al dipartimento delle imposte a Londra, National Audit Office . Un funzionario, contravvenendo ai regolamenti, avrebbe effettuato l'invio del materiale attraverso un comune corriere e i CD, come succede alla nostra posta ogni tanto, sono andati persi. Si è scatenata subito una caccia ai dati con tutti gli organi di sicurezza e

di polizia impegnati in ricerche a tappeto nelle scorse settimane, ma i due CD paiono essere letteralmente scomparsi senza lasciare alcuna traccia. I dati di 25 milioni di persone potrebbero finire nelle mani sbagliate, con conseguenze catastrofiche per la proverbiale difesa della privacy made in Britain. Il Ministero del Tesoro ha subito allertato banche e uffici finanziari, mentre i cittadini britannici sono stati invitati a vigilare sui movimenti dei propri conti in banca nelle prossime settimane. Il governo, presieduto da Gordon Brown, sta cercando in tutti i modi di evitare una nuova crisi bancaria, evitando che un panico incontrollato da parte dei clienti che ovviamente sono molto spaventati e iniziano a chiedere in blocco di cambiare conto corrente per tutelare la loro privacy e i loro risparmi. Il primo ministro ha chiesto ufficialmente scusa a nome del proprio governo per l'imperdonabile perdita dei due CD. Davanti alla Camera dei Comuni, Brown ha poi confermato di voler fare chiarezza sulla vicenda che ha portato alla più grave violazione dei diritti sulla privacy mai avvenuta in Gran Bretagna. Intanto, il responsabile del Tesoro Alistair Darling, pur confermando la gravità di quanto accaduto, ha difeso il proprio operato ricordando che i due CD dovrebbero essere dotati di una password e tutti noi sappiamo quanto questo sia un blocco da superare :-). Crackate le passowrd chiunque può accedere senza alcun problema alle informazioni contenute nei database che non sono neanche criptati. La cosa più comica, ma allo stesso tempo più tragica, è che per ovviare a questo tipo di problemi si sta cercando di accelerare il trasferimento di tutti i dati della pubblica amministrazione in rete il che sicuramente eviterebbe di perdere due CD ma, Dio ce ne scampi, porrebbe ben altri problemi si sicurezza informatica...

L'ASSALTO DEI MALWARE

Negli ultimi giorni di Novembre si è verificato uno dei peggiori attacchi malware che si ricodi portato avanti creando una catena di siti infetti che riescono sempre a piazzarsi tra i primi nelle ricerche di Google, Yahoo e simili grazie a una moltitudine di finti commenti con link e blog fantasma. Le chiavi di ricerca più pericoloso sono state per la maggior parte in inglese e quindi relativamente pericolose per l'Italia ma comunque è un fenomeno da tenere sott'occhio.

NO AL BULLISMO SU YouTube

All'indirizzo http://youtube.com/Beatbullying è nato un nuovo canale di YouTube contro il bullismo, molte le star, soprattutto della musica e dello sport che hanno lasciato il loro contributo video contro questo fenomeno che ormai balza agli onori delle cronache con una costanza allarmante. Continuano a ripetersi le segnalazioni di video che riguardano pestaggi di ragazzi diversamente abili, scene di bravate fatte a scuola ai danni dei compagni più deboli e via dicendo. Negli Stati Uniti questo fenomeno ha raggiunto dimensioni molto preoccupanti e YouTube ha deciso, anche perché spesso i video incriminati finiscono proprio sulle sue pagine, di fare qualcosa. Era ora!!!

TECNOSTRESSATI
ITALIANI UNITEVI!!!

Ogni tot salta fuori un nuovo male e a questo giro è toccato al tecnostres. I sintomi sono: perdita di concetrazione, ansia, affaticamento mentale, attacchi di panico, depressione, incubi e scatti di rabbia, praticamente l'identikit di ogni membro di questa redazione... Secondo un ricerca su circa 224 persone che passano di media 8/10 ore davanti al computer ogni giorno e i risultati sono che circa l'80% è risultato afflitto da questa sindrome data dall'overdose tecnologica. Siete tutti avvisati...

NAPOLI, LINUX,
NO GRAZIE!!!!

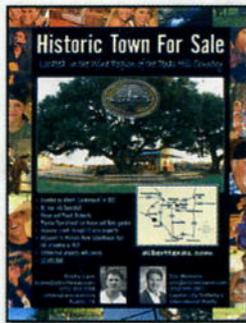
È una scelta che ovviamente non approviamo e sicuramente va in controtendenza con quello che sta succedendo in molti altri comuni ma il Comune di Napoli ha deciso di non fare il grande

HOT NEWS

JAVA AMA MAC OSX

Presto il sistema operativo made in Cupertino potrebbe diventare la piattaforma preferita dagli sviluppatori Java visto che è stata rilasciata una versione quasi completa del Java Development Kit 6 per Tiger e Leopard. L'implementazione permetterà ai programmatori di creare applicazioni Java 6 direttamente sul piattaforma Apple senza bisogno di Linux o Windows.

COMPRATI IL PAESE

Di roba strana su ebay se ne è sempre venduta tanta ma di vedere un paesino del Texas battuto all'asta non ce lo saremmo mai aspettati... Invece è successo e l'asta sembra essere stata vinta da un italiano, di cui ancora non è stato reso pubblico il nome, per 3.800.000 dollari. La notizia è stata confermata da chi il paese l'ha messo in vendita, l'agente immobiliare Bobby Cave. Da notare che il paese è praticamente formato solo da un paio di costruzioni e nulla più, cosa se ne farà il compratore è ancora tutto da capire.

FOTORITOCCO ONLINE

Ok, non è una roba nuova ma fa sempre piacere avere a disposizione nuovi strumenti on-line per fare i nostri giochi in liberta e senza dover installare software. Fotocrib.com è nato proprio per questo è ci permette di effettuare fotoritocchi senza bisogno di avere il costosissimo photoshop o altri applicativi. Quello che ci piace è il suo aspetto "minimalista, nella pagina avrete solo la foto da ritoccare e un menù a cascata con gli strumenti di cui avete bisogno per fare con le vostre foto ciò che volete.

Tribunale online

A Varese è stato deciso di aprire un sito che possa snellire le pratiche burocratiche del tribunale e il riperimento delle informazioni utili per accedere ai servizi del palazzo di giustizia. Si tratta oltretutto di un progetto che non costerà nulla alla pubblica amministrazione grazie alla collaborazione con l'ordine dei giornalisti e dei commercialisti.

salto verso l'opensource preferendo non rivoluzionare la sua rete informatica. E si che la proposta partiva da alcuni esponenti della maggioranza della giunta che prevedevano, grazie a questa mossa, di risparmiare fino ad un milione di euro in licenze software.

QUANTO COSTANO I CRACKER?

Secondo uno studio condotto da McAfee il costo sarebbe di miliardi di dollari. La ricerca di 40 pagine è stata realizzata in collaborazione con alcune agenzie governative e non come Nato, FBI, Soca, l'antiterrorismo Israeliano e la London School of Economics. Il panorama che ne esce è preoccupante, i cybercriminali restano impuniti e guadagnano miliardi inoltre internet sta diventando la prima forma, per importanza, di spionaggio politico, militare e industriale... Davvero una bella cartolina...

McAfee®

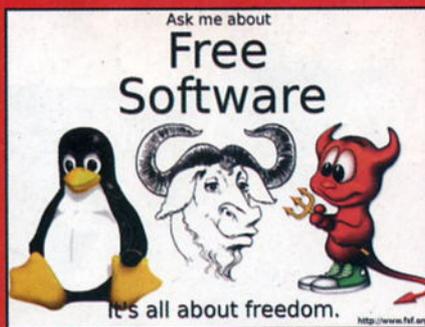
HOLLYWOOD VS CINA

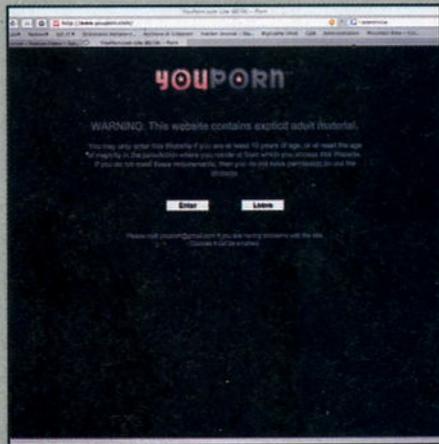
La Beijing Jeboo Interactive Science and Technology Company non è la prima volta che compare sulle pagine della nostra rivista, si tratta della compagnia proprietaria di jeboo.com, sito di distribuzione on-line di film. Questa volta il suo nome viene affiancato da un anonimo Internet Caffe di Shaghai nella causa intentata da Twentieth Century Fox Film Corporation, The Walt Disney Company, Paramount Pictures Corporation, Columbia Pictures Corporation, e Universal City Studios per aver distribuito film senza la loro autorizzazione. Secondo l'accusa l'Internet Caffe avrebbe messo a disposizione questi film attraverso un software sviluppato da Jeboo.com.

IL BUCO NERO DI INTERNET

Secondo i laboratori della DevLabs esisterebbe un mega bug nella struttura logico strutturale della rete e dei PC che se venisse scoperta da malintenzionati potrebbe scatenare un'epidemia di virus di nuova generazione difficilmente arginabile. La falla non sarebbe ne di un software ne di un sistema operativo e quindi non sarebbe possibile risolvere il problema con una patch. I nuovi virus agirebbero come un ricatto. Una volta infettato il PC di Pinco Pallino, il virus ricercherà tutti gli indirizzi email nel computer e si auto-invierà diverse volte. Se uno dei destinatari si lascerà infettare, il suo computer invierà in automatico una mail al PC di Pinco Pallino. Una volta ricevuta questa mail, lo worm toglierà dalla propria lista la mail del nuovo infettato. Fin qui è tutto nella norma ma chi rifiuterà di accettare questo virus, continuerà a ricevere mail infette. Solo installandolo, il mail-bombing avrà fine. Inoltre, sempre secondo gli esperti, questo tipo di worm non sarebbe arrestabile con i filtri antispam attualmente in circolazione grazie a un complesso intreccio di cript-decript che renderebbero le mail impossibile da bloccare.

DALLA PARTE DEL P2P

La Free Software Fundation fino ad ora se ne era tenuta fuori ma ora ha deciso che è il momento di agire e di schierarsi affianco agli utenti del P2P nelle battaglie legali che riguardano la violazione delle norme sul copyright. A questo punto la ormai famigerata RIAA di troverà contro una delle "istituzioni" del mondo informatico libero. La prima mossa è stata quella di iniziare il finanziamento della Expert Witness Defense Fund che sarà gestito in collaborazione con la Recordin Industry vs Polple e che interverrà ogni vola che spunteranno in qualche causa nomi come RIAA, Sony, BMG e compagnia bella.

PORNO 2.0

Il socialnetworking sta mietendo nuove vittime, si tratta del ricco e prosperoso mercato pornografico. La nascita di siti come YouPorn, Porntube e Xtube stanno difatti mettendo in ginocchio il vecchio giro d'affari dell'industria, nessuno compra più dvd e, tantomeno, videocassette e le vendite sono crollate negli ultimi 3 anni di circa il 50%. Dalla sua YouPorn raccoglie qualcosa come 15 milioni di utenti unici in un mese e fattura circa 2,4 milioni di dollari l'anno.

IPHONE 3G

Ebbene si!!! Una delle grandi perplessità riguardo l'arrivo in Italia dello smartphone di Apple era il fatto che supportasse solo la connessione Edge, la giustificazione era che il chipset 3G avrebbe occupa-

HOT NEWS

OCCHIO ALLE AGENZIE ON-LINE

Da un'iniziativa della Comunità Europea è sfociata un'inchiesta sulle frodi più ricorrenti in rete e il risultato è che bisogna tenere d'occhio le agenzie viaggio low cost. Pare infatti che queste abbiano la pessima abitudine di falsificare i dati sui costi effettivi delle offerte di viaggio nascondendo oneri aggiuntivi. Insomma ricordiamoci sempre che nessuno regala nulla e quindi davanti ad un'offerta troppo vantagiosa poniamoci sempre qualche domanda.

VI PREGO, UCCIDETE PIRATEBAY

Leggiamo, pubblichiamo e vorremmo non commentare:
"Esortiamo affinché venga condotta un'azione rapida e decisiva in Svezia contro uno dei maggiori player in Internet nella violazione del copyright"... stralcio della lettera inviata al ministro delle comucazioni svedese Asa Torstensson da: John Kennedy, presidente di IFPI, Alison Wenham, presidente di Worldwide Independent Network (WIN), Jonas Modig, presidente Federation of European Publishers (FEP) e tanti altri.

ALLA CACCIA DI MICROSOFT

Il suo nome è Saveer Bhatia ed è diventato famoso per aver creato, e poi venduto nel 1997 per una cifra "interessante", Hotmail ed ora è cofounder della società InstaColl che sta lanciando la sfida a Microsoft, proprio chi ha comprato Hotmail... Il terreno di gara è quello delle suite per l'ufficio Web-based e il prodotto di InstaColl è Live Documents. Certo si tratta di un mercato difficile e molto pieno se teniamo conto anche della presenza di Google Docs ma i nuovi arrivati garantiscono che il loro prodotto non è paragonabile anche per la possibilità di lavorare sia on-line che off-line, per la sua interfaccia userfriendly e per le funzionalità presenti.

Anoressia e Web

L'agenzia spagnola per il controllo di Internet ha richiesto e ottenuto dalla Microsoft la chiusura di 4 blog che incitavano all'anoressia e bulimia ospitate in Microsoft Windows Live Spaces. Riteniamo che sia uno step molto importante nella crescita della consapevolezza degli utenti della rete e anche nella lotta contro questo male che tante vittime sta facendo in tutto il mondo.

to troppo spazio e avrebbe anche significato un maggiore consumo della batteria ma ora questi problemi sembrano risolti e quindi nel 2008 dovrebbe arrivare la nuova versione con anche, secondo indiscrezioni, design più innovativo, una memoria interna da 16 Gb e GPS integrato.

FALLA IN QUICKTIME

Sembrerebbe che un buco del Viewer renda possibile il dirottamento di macchine Windows e Mac. Il problema è stato reso pubblico ed evidenziato con un attacco simulato creato da un professionista della security che come prima cosa ha studiato il problema (un bug già noto riguardo come QuickTime gestisce il Real Time Streaming Protocol) ed ha elaborato e pubblicato l'attacco per dimostrare alla Apple i punti deboli del suo software.
Il codice elaborato da Larry, il ricercatore in questione, è a prova d'errore e colpisce tutti i principali OS (Leopard, Vista e XP) come non accadeva da tempo, sfruttando un problema (la gestione dei flussi di dati audio/video in QuickTime) che ha già portato in passato a 4 tipi di attacchi diversi.

IL MULO silenzioso

Come diventare irrintracciabili durante l'uso dei programmi P2P

I software P2P che consentono l'anonimato (o, per meglio dire, che permettono di avvicinarsi ad una forma completa di anonimato) hanno come caratteristica saliente quella di nascondere l'indirizzo IP degli utenti che partecipano alla condivisione dei file. Per ottenere questo nelle operazioni vengono utilizzati degli indirizi fittizi, dalla conoscenza dei quali è poi molto difficile (se non praticamente impossibile) ricavare gli IP effettivi. Andiamo quindi a conoscere MUTE, una rete P2P anonima che fa a meno delle connessioni dirette tra utenti e sfrutta per il proprio funzionamento la crittografia asimmetrica. Cominceremo spiegando come installare ed utilizzare su Linux il client ufficiale per questa rete, presentando poi un client alternativo dalle caratteristiche interessanti.

:: Una rete P2P "muta"

Installiamo dunque su un PC Linux il programma Mute, nell'ultima release 0.5.1. Purtroppo non sono disponibili binari per le maggiori distribuzioni, quindi sarà necessario compilare manualmente il software. Per scaricare i sorgenti dal sito del progetto l'autore del programma richiede una piccola donazione: rimandando ad un momento successivo l'invio di denaro (se lo desideriamo), possiamo comunque prelevare il pacchetto che ci serve da un altro indirizzo, ad esempio da http://tinyurl.com/36xb89. Ciò è perfettamente in linea con la licenza libera di Mute. Ottenuto il pacchetto dei sorgenti, quindi, scompattiamolo (comando "tar xvfz MUTE_fileSharing-0.5.1_UnixSource.tar.gz") ed entriamo nella directory appena creata. La compilazione del programma richiede la presenza dei

▲ *MUTE utilizza wxWidgets per l'interfaccia. Attenti ad installare la giusta versione della libreria!*

file di sviluppo della libreria wxWidgets: assicuriamoci di avere nel nostro sistema la versione 2.4 di questa, le successive release della libreria, infatti, non riusciranno a condurre in porto la compilazione (su Ubuntu 7.10 il pacchetto da installare è libwxgtk2.4-dev).

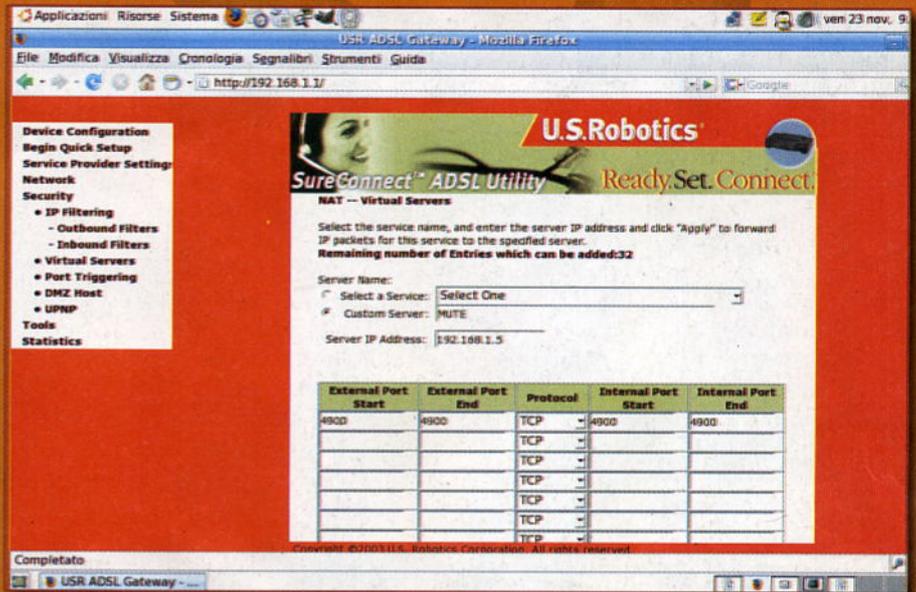
:: La procedura per una corretta compilazione

A questo punto avviamo la compilazione eseguendo in console "./runToBuild". Ci verrà richiesto di selezionare la piattaforma della nostra macchina: scegliamo "1" (GNU/Linux X86). Ora dovremo inserire il percorso del programma wx-config;

Per compilare MUTE dobbiamo rispondere ad alcune semplici domande...

individuiamo quale sia aprendo una seconda console e lanciando "which wx-config". L'output di questo comando corrisponderà al path completo di wx-config. Torniamo alla console iniziale. Se il percorso indicato da which è /usr/bin/wx-config, battiamo semplicemente Invio in risposta alla seconda domanda; in caso contrario inseriamo il path completo. Alla terza domanda rispondiamo con "1", così da compilare il programma completo di interfaccia grafica. Al termine della compilazione troveremo l'eseguibile di MUTE, fileSharingMUTE, nella sottodirectory MUTE_GUI_fileSharing.

:: Installazione

Rendiamo scrivibile da tutti gli utenti la cartella MUTE_GUI_fileSharing mediante il comando "chmod a+w MUTE_GUI_fileSharing/" e, come ultima finezza, riduciamo drasticamente le dimensioni del programma che abbiamo appena compilato con "strip MUTE_GUI_fileSharing/fileSharingMUTE". A questo punto, per lanciare MUTE ci basterà aprire una console, entrare nella directory MUTE_GUI_fileSharing e lanciare "./fileSharingMUTE". Per poterci connettere agli altri nodi della rete dobbiamo inserire degli 'host caches' aggiornati; per fare questo, apriamo con un editor il file MUTE_GUI_fileSharing/settings/webHostCaches.ini, cancelliamone l'intero contenuto ed inseriamo nel file gli indirizzi segnalati nella pagina web http://mute-net.sourceforge.net/quickStartGuide.php (il primo indirizzo dell'elenco è http://mutecache.ath.cx/mcache.php). A questo punto, prima di connetterci è consigliabile aprire sul firewall attivo sul nostro sistema (ad esempio quello presente sul router) la porta 4900; MUTE funziona perfettamente senza aprire alcuna porta, ma trovare dei nodi con cui connettersi in questo caso sarà più difficile (la connessione, infatti, non può avvenire tra due nodi sotto firewall).

Apriamo sul firewall del nostro router la porta 4900.

```
http://mutecache.ath.cx/mcache.php
http://mcache.guenever.net/mcache.php
http://mcache.northcountrynotes.org/mcache.php
http://mcache.naskel.cx/mcache.php
http://mute.filesharinghelp.com/mcache.php
http://www.mymute.net/mutewebcache/mcache.php
http://mboardy.mb.ohost.de/m/mcache.php
http://mcache.mc.funpic.de/mcache.php
http://reezer.freeshell.org/mcache/mcache.php
http://mcache.freehostia.com/mcache.php
```

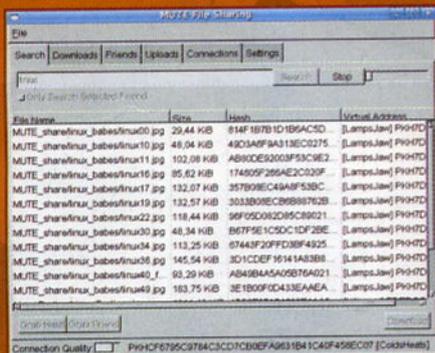
Il contenuto del file webHostCaches.ini deve essere questo.

:: Il programma al primo avvio

La prima volta che lanciamo MUTE ci vengono poste alcune domande. La prima riguarda la presenza di un firewall che blocca le connessioni in entrata per MUTE: dato che abbiamo aperto la porta 4900, clickiamo su "No". Poi dobbiamo inserire dei caratteri casuali sulla tastiera per rendere più sicura la chiave di crittazione che verrà creata; quindi indichiamo le dimensioni della chiave stessa: lasciamo il valore di default, 1024 bits. Infine, selezioniamo la directory che vogliamo condividere nella rete MUTE. A questo punto comparirà la finestra del programma. Verranno tentate

connessioni con gli altri nodi e sarà necessario pazientare un poco prima di poter effettivamente entrare nella rete.

:: Ricerche nella rete

Nella finestra del progamma clickiamo sulla linguetta "Connections": qui vengono elencati i nodi a cui siamo connessi. Una volta collegati ad almeno un nodo, passiamo alla linguetta "Search": in questa sezione dell'interfaccia possiamo effettuare ricerche nella rete. MUTE consente ricerche solo per sottostringhe; possiamo, ad esempio, scrivere txt per ricercare file terminanti con il prefisso .txt o iso per individuare immagini ISO nella rete. Trovato il file che ci interessa scaricare, selezioniamolo nell'elenco e clickiamo quindi sul pulsante "Download" in basso. Il download in anonimato avrà inizio!

Con MUTE possiamo effettuare ricerche nella rete mediante delle semplici sottostringhe

:: Download automatizzati con NapShare

NapShare è un client per reti MUTE con alcune interessanti funzionalità aggiuntive rispetto al client ufficiale: permette, infatti, di effettuare scaricamenti automatici e di ripristinare i download dei file in caso di interruzione. Per installare NapShare andiamo sul sito del programma e scarichiamo il pacchetto dei sorgenti; derivando il programma dal client MUTE, la procedura di compilazione è la medesima. Seguiamo quindi le istruzioni riportate per la compilazione di MUTE, con l'accortezza di utilizzare la versione 3.4 del compilatore g++ (versioni successive, infatti, daranno errori nella creazione dell'eseguibile). Se usiamo una distro derivata da Debian, come Ubuntu, per installare questa release di GNU C++ otteniamo i permessi di root (comando "sudo -s" in Ubuntu, "su -" in Debian) e digitiamo "apt-get install g++-3.4"; poi eseguiamo "rm /usr/bin/g++" e, successivamente, "ln -s /usr/bin/g++-3.4 /usr/bin/g++". In seguito, per ritornare ad usare l'ultima versione di GNU C++ lanciamo "rm /usr/bin/g++" e "ln -s /usr/bin/g++-4.1 /usr/bin/g++".
Al termine della compilazione, quindi, troveremo il binario di NapShare, anch'esso chiamato fileSharingMUTE, nella cartella MUTE_GUI_fileSharing contenuta nella directory dei sorgenti (NapShare_2_2_4_Source).

:: Lanciamo NapShare

Al primo avvio di NapShare dovremo fornire le stesse informazioni richieste dal client MUTE. Anche l'interfaccia grafica dei due software è molto simile. La differenza più vistosa è la presenza della linguetta "Automation", che controlla gli scaricamenti automatizzati. Si tratta di una funzionalità che consente di stabilire nella configurazione di NapShare alcuni criteri di ricerca, utilizzando parole chiavi e filtri: il programma andrà quindi a caccia nella rete, inserendo in automatico nella coda di download tutti i file che soddisfano tali criteri. Il file di configurazione su cui intervenire per abilitare tale funzionalità è MUTE_GUI_fileSharing/settings/NAPS-auto.ini. Apriamo questo file con un editor di testi: le righe che ci interessano sono quelle che iniziano con "list_" (cancelliamo tutte le linee di questo tipo che troviamo nel file, si tratta infatti di righe di esempio). Ora costruiamo un semplice criterio di ricerca, che scarichi in automatico tutti i file i cui nomi contengano la parola 'linux' ma che non siano né immagini JPEG né file ZIP; ecco le due linee che ci servono:
list_strings = "jpg jpeg zip"

list_search = "linux"
Le due righe possono essere tradotte così: cerca (list_search) tutti i file con la parola "linux", scartando (list_strings) i file contenenti le parole jpg, jpeg e zip. Inseriamo le linee in NAPS-auto.ini, lanciamo NapShare e nella linguetta "Automation" clickiamo sul pulsante "Start Automation". Sguinzaglieremo così il nostro... segugio nella rete anonima. ■

http://mute-net.sourceforge.net/
http://napshare.sourceforge.net/,

Per attivare il download automatico dobbiamo modificare un file di configurazione

Una volta creati i nostri criteri di ricerca non ci rimane che clickare su "Start Automation"...

Pubblicità INFETTA

Sembrerà strano ma anche i banner possono essere un vero pericolo per il nostro PC

Mai fidarsi! Il famoso motto sembra più che mai appropriato quando si naviga in Internet, perché ormai le minacce si nascondono dietro ogni angolo. Se per esempio cliccando su un banner appare improvvisamente un messaggio che ci avverte che il nostro computer è infetto, offrendoci una rapida soluzione in cambio di denaro e dei dati della nostra carta di credito, facciamo attenzione: è una trappola! Non solo non risolveremo alcun problema, che in realtà spesso neanche esiste, ma ci ritroveremo con il computer infettato e con i dati della nostra carta di credito a disposizione di qualche malintenzionato. La colpa di questi episodi va spesso attribuita alla negligenza di chi gestisce il sito, che non aggiorna i sistemi di difesa, permettendo così l'inserimento di codici maligni all'interno di banner pubblicitari.

Don Jackson, un ricercatore di SecureWorks, azienda che si occupa di sicurezza informatica, ha precisato che questo fenomeno riguarda soprattutto siti "al di sopra di ogni sospetto e molto frequentati". Lo scopo naturalmente è sempre il solito: truffare gli utenti più sprovveduti e prendere possesso a distanza dei loro computer senza che se ne accorgano. I siti più colpiti sono quelli che riguardano l'intrattenimento online, anche perché sono quelli più visitati dagli utenti meno esperti.
Ma chi sono i veri colpevoli di questa situazione? Difficile dirlo, perché è proprio il sistema stesso a essere molto complesso. Infatti per inserire i banner i siti si rivolgono a ditte pubblicitarie, le quali si rivolgono a loro volta ad aziende più piccole per la realizzazione. Quindi è come cercare il classico ago nel pagliaio...

Per fortuna abbiamo qualche metodo piuttosto semplice per difenderci. Con Firefox possiamo scaricare e usare l'estensione noscript, mentre con Internet Explorer possiamo attivare la funzione di blocco dei pop-up, nel menu Strumenti. Tuttavia l'arma migliore resta la cautela e imparare a non fidarsi anche dei siti più famosi. Sappiamo bene che coloro che creano questi codici maligni cercano di essere sempre un passo avanti per trovare metodi sempre più subdoli per aggirare i nostri sistemi di difesa, quindi diffidiamo sempre di chi ci promette di risolverci i problemi da un sito Internet in cambio di qualche decina di dollari. ■

ANTIPIRATERIA alla francese

"Corriamo il rischio di essere testimoni della distruzione della cultura. Internet non deve diventare un Far West di alta tecnologia, una zona senza normative dove i fuorilegge possano sottrarre le opere dell'ingegno senza farsi problemi o, peggio ancora, venderle nella più assoluta impunità. E sulle spalle di chi? Sulle spalle degli artisti"
Nicolas Sarkozy

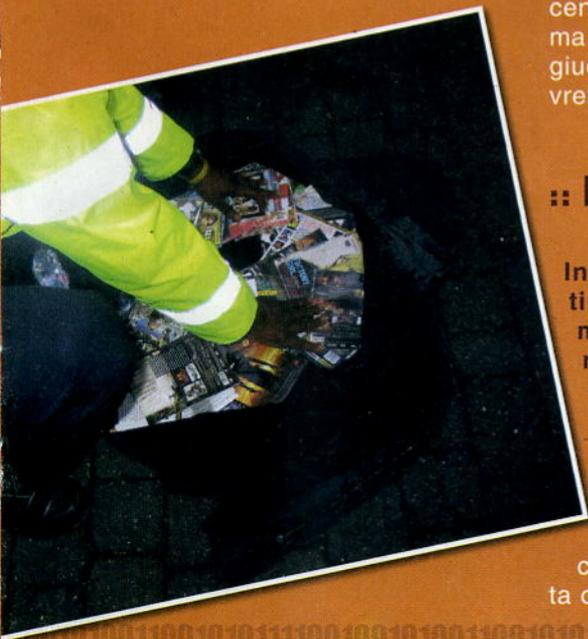
La ricetta arriva direttamente dal presidente della Repubblica Francese Nicola Sarcozy che ha deciso di mettere un fine al fenomeno della pirateria in Francia.
I presupposti per questa azione così drastica sono gli accordi incrociati tra major e provider con l'appoggio di multinazionali della distribuzione di audio e video tra cui il boss di FNAC, Denis Olivennes.

:: Il primo passo

Tutto è cominciato con l'istituzione di una Autorità Anti-Pirateria che si occuperà di distribuire sanzioni ai detentori delle connessioni dove si verificassero abusi del diritto d'autore. L'Autorità sarà soggetta al magistrato in modo da garantire la legittimità dei sui interventi. Una volta ricevuto il beneplacito del magistrato si procederà ad inviare, tramite il provider, una comunicazione al trasgressore, dopo tre di questi avvisi la connessione interenet può anche essere chiusa in maniera coatta. Ovviamente tutti abbiamo pensato, beh, io cambio provider e vado avanti... ma è stata prevista la realizzazione di una lista nazionale dei pirati, ossia di quegli utenti i cui abbonamenti siano stati terminati in base a questo provvedimento.

:: E la privacy???

Il problema in questi casi, e si tratta di ben più di un problema, è la salvaguardia della privacy degli utenti della rete, in definitiva l'Autorità Anti-Pirateria ha il diritto di monitorare le reti di sharing cosa che da noi, in Italia, è fonte di molte discussioni, ricordiamo tutti i il recente caso Peppermint. Per permettere questo scanning, e soprattutto per garantirsi "'l'aiuto" dei provider, l'Autorità potrà rivalersi anche su questi nel caso non mettano in atto tutte le misure per arginare il fenomeno e non collaborino nello stanare i "pirati". Ovviamente è stata anche snellita la procedura per

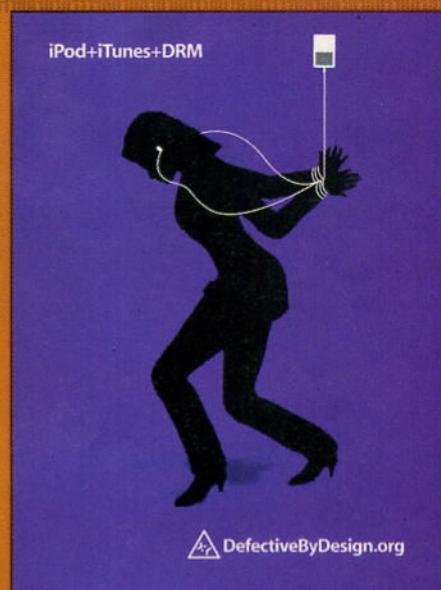
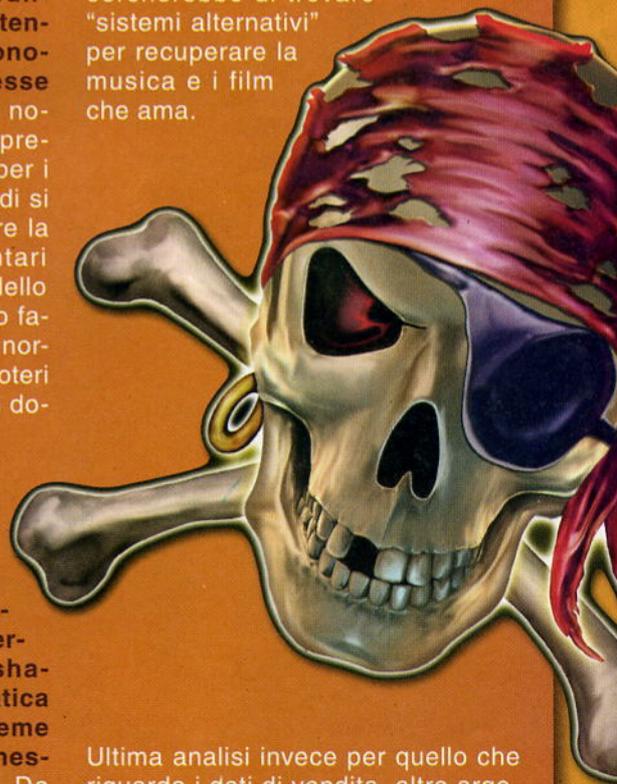
il sequestro dei server sospettati di ospitare servizi di sharing o sistemi e servizi che possano essere utilizzati per scaricare materiale coperto da copyright, capite tutti benissimo che significa che ogni server, o quasi, è a rischio sequestro. Di buono c'è che senza la sentenza di un magistrato non potranno essere chiusi servizi di anonimato e privacy, certo che se la legge va in questa direzione possiamo immaginare da che parte penderanno le sentenze d'ora in poi.

:: A favore...

Ovviamente i "tromboni" delle major non hanno perso l'occasione per alzare i loro vessilli. Primo fra tutti John Kennedy, boss dell'IFPI (federazione internazionale dei fonografici) che ha definito questa come una delle normative più all'avanguardia per la vittoria contro la pirateria on-line. Ci mancherebbe anche che non fossero felici, hanno finalmente ottenuto il coinvolgimento dei provider...

:: Contro...

Semplici, chiare e dirette le affermazioni di UFC-Que Choisir, importante associazione dei consumatori, che ha definito i punti del progetto "molto duri, potenzialmente repressivi, anti-economici e diretti contro le promesse dell'era digitale". Si fa inoltre notare che la legge francese già prevede fino a tre anni di carcere per i casi più gravi di pirateria e quindi si poteva anche evitare di inasprire la norma. Anche i due parlamentari Marc Le Fur e Alain Suguenot, dello stesso partito di Sarkozy, stanno facendo pressioni contro la nuova norma ritenendo che vengano dati poteri giudiziari ad un'agenzia che non dovrebbe detenerli.

:: In fine

Insomma ci troviamo davanti all'ennesimo tentativo di fermare il fenomeno del filesharing demonizzando una pratica che, di per sé, nasce assieme ad internet e che non ha nessun connotato negativo. Da parte nostra vorremmo che per prima cosa si facesse qualcosa contro la vera pirateria, quelle che masterizza milioni di CD pirata ogni hanno è che mette sui nostri

marciapiedi DVD con i film che ancora devono uscire in sala. Inoltre vorremmo anche, per l'ennesima volta, far notare che, forse, con un prezzo dei CD più basso la gente non cercherebbe di trovare "sistemi alternativi" per recuperare la musica e i film che ama.

Ultima analisi invece per quello che riguarda i dati di vendita, altro argomento che trattiamo con una costanza allarmante, siamo sicuri che i dati pubblicati nelle varie ricerche (per lo più finanziate da IFPI e analoghi) corrispondano alla realtà???

La posta infinita

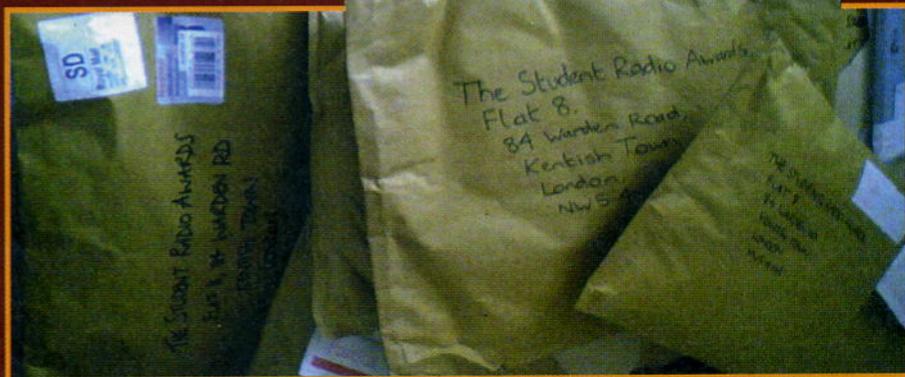
Per spam si intende l'invio di grandi quantità di messaggi promozionali indesiderati. Attualmente circola spam ovunque: nelle email, nelle cassette delle lettere, negli sms, solo per citare i casi più eclatanti.

Il principale sistema utilizzato per lo spamming rimane comunque internet. Si stima che circa i 2/3 delle email che circolano quotidianamente in rete siano di contenuto indesiderato. È infatti semplicissimo programmare uno script che crei una una wordlist di nomi del tipo:

"anna, barbara, roberto, guido, evelina...."

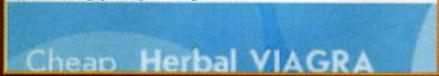
associando poi questi nomi comuni a domini che forniscono servizio di webmail (es. "gmail.com", "libero.it"...) è possibile creare un database di centinaia di migliaia di indirizzi, da verificare, ma comunque presumibilmente validi. Se utilizzassimo un sistema un po più complicato ed associassimo ad una wordlist anche dei caratteri numerici, riusciremmo ad ampliare ulteriormente la nostra sourcelist di indirizzi.

Questo è solo uno dei sistemi utilizzato per creare le cosiddette "spamlist" o "spamarchive". È infatti doveroso sottolineare che esistono veri e propri gruppi di cracker che vendono allo spammer miglior offerente, liste con centinaia di migliaia (se non milioni) di email valide, solitamente rubate tramite GoogleHacking o grazie alla forzatura di database di forum e di servizi di newsletter.

Fortunatamente gli attuali internet provider ed i programmi di gestione delle e-mail, utilizzano sistemi di filtraggio automatico dei messaggi per la posta indesiderata; il più famoso modello statistico/matematico utilizzato in questo ambito è chiamato sistema "Bayes", che risulta essere la miglior alternativa rispetto alle classiche "black list".
Il filtro "bayesiano" prende il nome da un noto matematico inglese vissuto nel diciottesimo secolo che elaborò una regola statistica per la quale ad ogni evento è attribuita una probabilità. Applicando il modello al problema dello spam possiamo dire in maniera generica che se in un numero n delle mail analizzate precedentemente, l'utente ha marcato come spam quelle che contenevano la parola "sex", il filtro ne dedurrà che la presenza di quella parola innalza la probabilità che le mail seguenti contenenti quella parola siano a loro volta spam. In questo modo, l'applicazione è in grado di adattarsi in maniera dinamica e veloce alle nuove tipologie di

spam cosa che non accadeva utilizzando le comunissime "black list". Queste ultime infatti funzionano individuando una parola indesiderata nel testo o nell'oggetto del messaggio eliminandola definitivamente. Ciò provoca alcuni problemi: supponendo di eliminare i messaggi con in oggetto la parola "sex", avremo da un lato l'eliminazione dei soli spamming di tale tipologia, dall'altro non riceveremo ad esempio una mail scherzosa di un conoscente.

Gli spammer cercano di aggirare questi filtro utilizzando alcuni stratagemmi. Andiamo ad analizzare alcuni casi:

lay at Patriarch's Ponds, but they did not pay much attention to it and silence. He took Ivan's temperature, felt his pulse and looked into his though not painfully, traced some signs on the skin of his chest with th t, pricked his elbow joint, wrapped rubber bracelets round his arm . hem from the mysterious professor, and had tried to catch him, yet al Vologda. At last they let Ivan go. He was led back to his room where sdjksdfsdfsdlgkj sdflkjsdf lksdjfsdfsdf

Cheap Herbal VIAGRA

In questa email come potete vedere, vengono inserite nel testo iniziale delle parole o frasi che non sono inerenti al vero contenuto della mail (cercando in questo modo di sviare il sistema di bayes)

Rolex
Cartier
Bvlgari
Franck Muller
Patek Philippe
Vacheron Constantin
A.Lange & Sohne
Audemars Piguet
Jaeger-Lecoultre
IWC
Officine Panerai
Breitling
Omega
Tag Heuer

Just example

ROLEX
Full 18K Gold
Daytona for MEN
OUR PRICE $269

In questo caso il messaggio di spam viene inserito direttamente all'interno di una immagine gif o jpg in modo tale da non rendere possibile un' analisi dei vocaboli con il sistema statistico.

Orderinq Viaqra online is a very convinient ,fast and secure way! Millions of people do it daily to save their privacy and money

Ecco qui l'ultimo caso che andiamo ad analizzare. Come potete vedere all'interno dell'immagine vengono utilizzate appositamente parole non corrette (in questa immagine per esempio nella parola "Orderinq" è stata sostituita l'ultima lettera etc..

Esiste ancora, un sistema più articolato e complesso che permette ad un individuo malintenzionato di offuscare completamente un URL di destinazione. Questa tecnica è anche utilizzata da phisher in cerca di informazioni sensibili quali credenziali di accesso, cookies, numeri di carte di credito, per rendere più difficile il filtering di questo tipo di attacco.

Come ben saprete un sito internet può essere visualizzato digitando sia il nome dell'host nella barra degli indirizzi (es. www.google.it) sia digitando l'indirizzo IP corrispondente, in questo caso: http://216.239.59.103/ (a meno che ovviamente non risiedano più host su uno stesso indirizzo IP). Un comune indirizzo IP (di versione IPV4) è formato da 4 serie di numeri compresi tra 0 e 255 separate tra loro da punti. Andiamo ora a convertire questo indirizzo, nel sistema numerico esadecimale sfruttando una comune calcolatrice scientifica:

216 ---> 0xd8
239 ---> 0xef
59 ---> 0x3b
103 ---> 0x67

Utilizzando il sistema esadecimale, il nostro indirizzo IP diverrà quindi: http://0xd8.0xef.0x3b.0x67/

È possibile poi, effettuare la stessa operazione sfruttando il sistema "ottale": http://0330.0357.073.0147/

I browsers riescono quindi a risolvere un indirizzo IP, a prescindere dal sistema metrico utilizzato ed eliminando eventuali cifre superflue (come lo zero). Usando questo "mix di compatibilità" è estremamente facile creare un indirizzo IP completamente occultato rispetto all'originale in modo da riuscire ad eludere il nostro fedele filtro antispam...

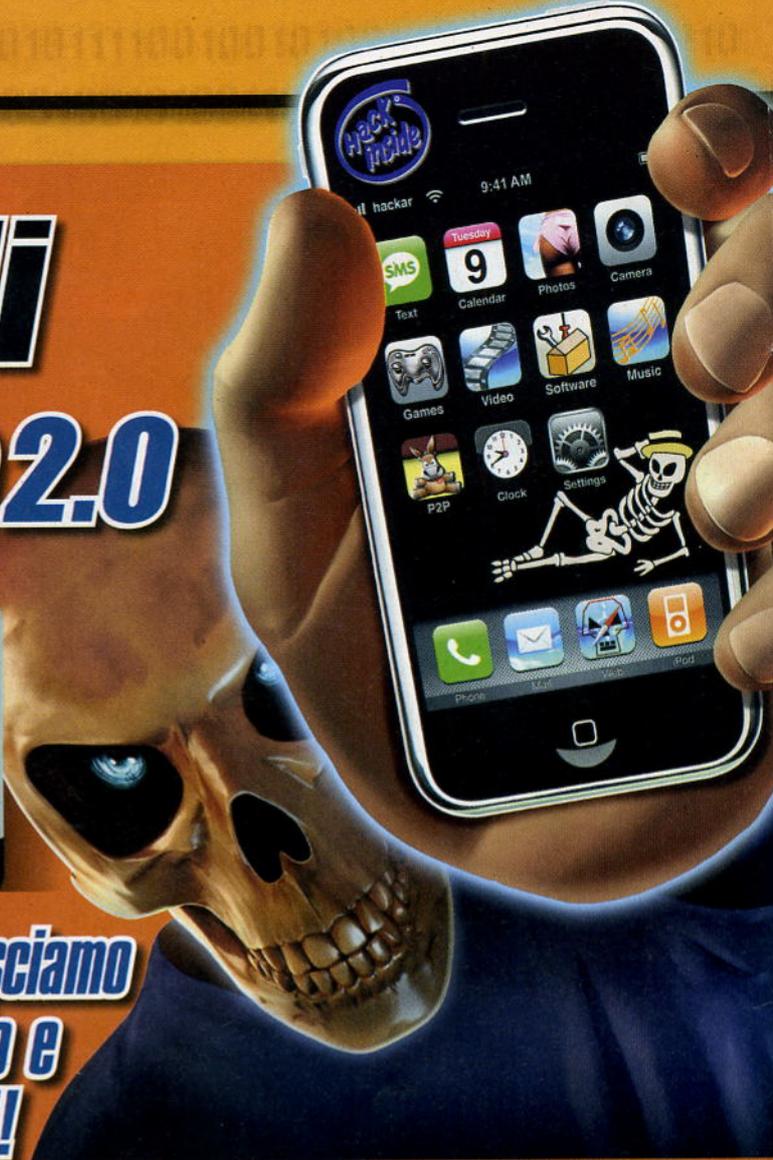
Chi mi sa dire a che sito si riferisce questo link?

http://0x00000d4.000102.0x00000000068.00068

Buon hacking a tutti!

LINK BOX

http://it.wikipedia.org/wiki/Filtro_bayesiano
http://becomingparanoid.com/2006/03/29/e-mail-security-detecting-spam-ii/
http://support.gfi.com/manuals/it/me11/me11manual_it-1-12.html
http://exploit.blogosfere.it/
http://it.wikipedia.org/wiki/IPv4

Crack di iPhone 2.0

Se siamo deboli di cuore, lasciamo perdere, perché è complicato e pericoloso... Ma che risultati!

Come va l'iPhone? È la domanda che ci facciamo tutti, anche se per ora il nuovo smartphone di Apple non è venduto in Italia. Siamo però riusciti a procurarcene uno e abbiamo subito inserito una comune SIM. Ebbene, funziona! Naturalmente c'è il trucco, non solo perché l'iPhone per ora è solo un bel soprammobile senza un contratto telefonico con l'operatore americano AT&T.

:: Lo sblocco in 5 mosse

Quando lo tiriamo fuori dalla scatola, l'iPhone non sa fare niente: non telefona, non naviga in Internet, non serve da assistente personale. Prima di tutto, dobbiamo installare su un computer il programma fornito da Apple e collegare l'iPhone con un cavo USB.

• Dobbiamo usare iTunes, il programma di sincronizzazione noto ai possessori dell'iPod, che serve a "svegliare" l'iPhone. Ma se non abbiamo sottoscritto l'abbonamento con At&T, la storia finisce qui... in teoria.

• In pratica, per raggirare iTunes, prima di collegare l'iPhone al computer, dobbiamo avviare un programma creato dall'hacker norvegese Jon Lech Johansen, più conosciuto con lo pseudonimo di DVD Jon.
A questo punto possiamo attivare l'iPhone senza abbonamento ad AT&T, ma solo per le funzioni iPod, Wi-Fi, programma di navigazione Internet e fotocamera.

• Per attivare il telefono, dobbiamo usare un altro programma chiamato iUnlock, sempre di origine norvegese. Si tratta di un pacchetto di programmini che dobbiamo lanciare sul nostro computer in

CHE RISCHIO!

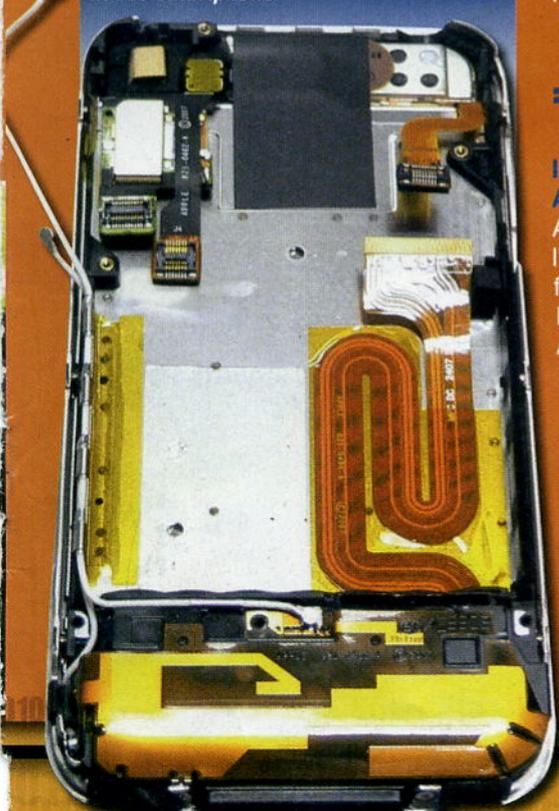
Attenzione, il procedimento di attivazione usato sul nostro iPhone non è gradito a Apple, quindi non aspettiamoci che venga mantenuta la garanzia. Comunque possiamo dire che la procedura, di cui abbiamo descritto il principio, è stata condotta con successo sull'iPhone che abbiamo avuto tra le mani e che il gioiello si comporta bene perché funziona perfettamente. Ciò che non possiamo garantire è che tutto funzioni altrettanto bene con altri iPhone, trasformandoli così in oggetti completamente inutili. Temiamo comunque che i prossimi aggiornamenti ufficiali del sistema operativo dell'iPhone cancelleranno gli effetti dell'operazione che abbiamo fatto. Ciò che pubblichiamo non sono istruzioni per l'uso, ma solo una semplice testimonianza.

Ovviamente è già possibile trovare i "cloni" cinesi dell'iPod ma non garantiamo sulla qualità del prodotto...

modalità riga di comando. La procedura, interrotta da vari riavvii dell'iPhone, dura circa mezzora.
Alla fine, dobbiamo solo installare dei file complementari perché l'iPhone parli italiano. Comunque la sua tastiera resta in modalità Qwerty.

• Da questo momento, il nostro iPhone funziona con l'abbonamento della SIM che abbiamo inserito, indipendentemente dall'operatore.

Ecco cosa succede a grandi linee, ma facciamo attenzione e calcoliamo bene la difficoltà dell'operazione: le procedure descritte in inglese sono molto difficili per i comuni mortali!

Ecco cosa si nasconde dentro il nostro nuovo smartphone

:: Possiamo già comprarlo?

In pratica, per ora da noi il gioiellino di Apple è inutilizzabile.
A meno che... Diciamolo chiaramente, l'iPhone non può essere comprato al di fuori degli Stati Uniti, cosa che non è alla portata di tutti. Dobbiamo andare in un Apple Store (un punto vendita di Apple) e specificare che lo copriamo per regalarlo. In questo modo non saremo obbligati a sottoscrivere un abbonamento con AT&T (minimo 60 dollari al mese per un periodo di due anni), visto che vogliamo usarlo con la nostra SIM. Dopo il recente ribasso annunciato da Apple, usciremo da uno dei suoi punti vendita con un iPhone a 399 dollari, cioè circa 295 euro. Un risparmio di almeno 100 euro, rispetto ai costi previsti in Italia!

:: L'anima Unix è una buona occasione

Il fatto che si possa intervenire sul programma dell'iPhone è un buon segno perché, dopo aver sbloccato l'apparecchio, è possibile installare con lo stesso metodo i programmi che non provengono dal mondo Apple.

GLOSSARIO

• 3G
Sigla che accompagna i cellulari di "terza generazione", gli UMTS. Offre nuovi servizi come la videofonia, l'accesso veloce a Internet dal telefonino e opzioni video (televisione in diretta o filmati da scaricare).

• Edge
A metà strada tra il GPRS e il 3G, Edge offre un collegamento veloce a Internet con un cellulare. Ecco perché viene soprannominato 2,75G. In teoria, Edge raggiunge una velocità di 250 kbit/s, in pratica va alla metà.

• Flash
Formato di animazione usato in Internet. Le animazioni Flash sono di solito inserite in pagine Web e lette direttamente dal programma di navigazione (Internet Explorer, Firefox, Opera o altri). Bisogna però scaricare il programma gratuito Flash Player.

• Multipoint
Diversamente dagli altri PDA, lo schermo dell'iPhone riesce a riconoscere il tocco contemporaneo di più dita. Questa funzione, integrata all'elettronica dello schermo, permette anche a produttori come Apple di offrire nuovi usi, per esempio lo zoom di un'immagine.

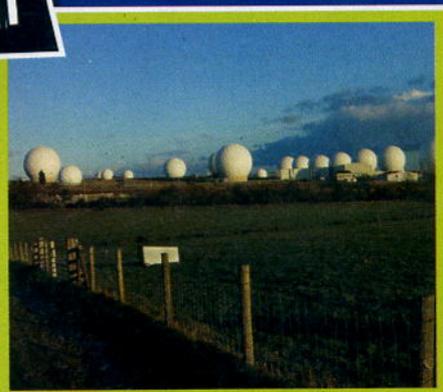
Siccome il "cuore", cioè il centro del sistema operativo dell'iPhone, è Unix, siamo pronti a scommettere che la comunità degli sviluppatori Linux saprà creare nuovi interessanti applicazioni.
Per ora, possiamo solo constatare che se vogliamo sfruttare le possibilità del nostro telefono dobbiamo affrontare procedure molto complicate, ma con un po' di pazienza, tutto dovrebbe diventare più facile. ■

LA SPIA che veniva DA INTERNET

Esiste il "Grande Fratello"? Qualcuno ci spia tramite il nostro PC? O forse grazie ai cellulari? Ecco come possiamo difenderci dalle attenzioni indesiderate!

La seconda metà del ventesimo secolo è stata caratterizzata da un notevole aumento di paura generalizzata, in un atteggiamento che ha raggiunto anche casi di autentico isterismo. Siamo tutti preoccupati dal fatto che ci sia un grande occhio controllore che tenga sotto controllo la nostra identità, le nostre azioni o persino i nostri pensieri. Ma c'è effettivamente qualcosa di vero in tutto ciò? E se le cose stanno così, come possiamo fare per mantenere il più possibile la nostra privacy?

INSTALLAZIONI

Echelon dovrebbe vantare numerose e costosissime installazioni in tutto il mondo. Secondo i rapporti, infatti, si parla di più di 50 stazioni di ascolto in tutto il mondo, compresa la base dell'aeronautica di San Vito dei Normanni, in provincia di Brindisi (chiusa nel 1994) e altre basi simili in Germania, Spagna, Regno Unito, Francia, Danimarca, Cipro, Malta, Turchia, eccetera.

:: Il mistero di Echelon

Ci sono numerose voci e leggende riguardanti Echelon, una supposta rete internazionale segretissima di ricerca, scambio ed elaborazione delle informazioni che terrebbe sott'occhio ogni nostro movimento tramite i computer, i cellulari, le carte di credito, eccetera. Si dice che tale rete sia sotto il controllo della Comunità UKUSA, a capo della quale ci sarebbero le agenzie di intelligence di cinque nazioni anglosassoni (Australia, Canada, Nuova Zelanda e, soprattutto, Stati Uniti e Regno Unito). Attenzione: non stiamo parlando di semplici leggende metropolitane! I dati qui riportati sono stati ripresi anche da rapporti ufficiali della Comunità Europea, come è accaduto nel 2001.
L'esistenza di Echelon è stata rivelata la prima volta da Duncan Campbell, un giornalista investigativo freelance, nonché produttore televisivo, in un articolo pubblicato sulla rivista inglese New Statesman nel 1988, intitolato Someone's Listening, in italiano: qualcuno sta ascoltando. Secondo questo articolo e numerosi altri rapporti e racconti provenienti dalle fonti più disparate, Echelon potrebbe facilmente captare comunicazioni satellitari e radio, conversazioni telefoniche, fax, messaggi di posta elettronica e altro ancora, e sarebbe in grado di catalogare ogni informazione ricevuta in modo del tutto automatico, mantenendo l'attenzione solo su una serie di parole chiave che risultano "calde". A bilanciare molte affermazioni scandalistiche spesso eccessive, possiamo dire che il Comitato della Comunità Europea che ha indagato sul fenomeno e che ha pubblicato il rapporto di cui abbiamo parlato poco fa, ha concluso che le reali capacità tecniche di un simile sistema sono, in realtà, molto più limitate di quanto farebbero pensare le incontrollabili "voci di corridoio". Tali capacità, comunque, suonano piuttosto preoccupanti anche a un esame realistico. Le trasmissioni radio ad alta frequenza (chiamate anche onde corte) sono, effettivamente, intercettabili facilmente anche a grande distanza. L'installazione di satelliti specifici per facilitare le comunicazioni e le trasmissioni audio/video rende possibile mantenere un registro aggiornato praticamente in tempo reale di qualsiasi tipo di messaggio passi per tali satelliti: telefonate, fax, email, traffico di dati, trasmissioni televisive, radiofoniche e molto altro. Le trasmissioni a voce e di dati, però, al giorno d'oggi passano al 99 percento tramite collegamenti in fibre ottiche. Questo rende l'intercettazione molto meno comoda: è necessario installare stazioni di ascolto sulle linee delle fibre ottiche stesse, rendendo le capacità di controllo di Echelon molto più limitate rispetto ai decenni passati.
Echelon, dunque, è una realtà, non una leggenda, anche se molto probabilmente non si occupa di controllare l'intera popolazione mondiale come una specie di super "Grande Fratello", ma soltanto alcune "zone calde" e alcuni tipi di comunicazione.

Good evening ! How has your day been!

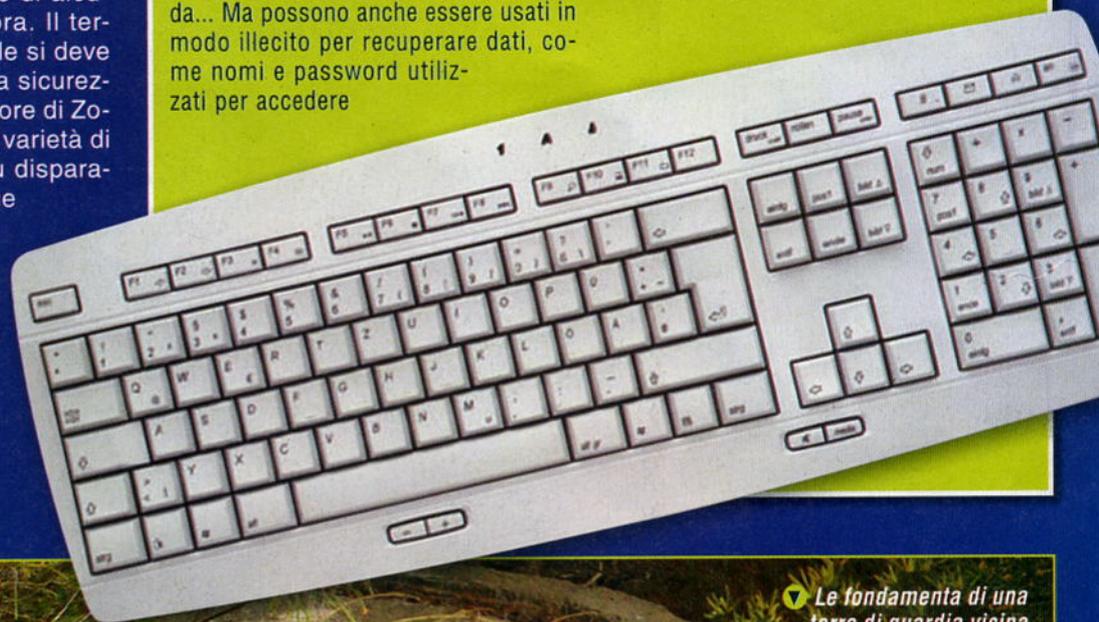
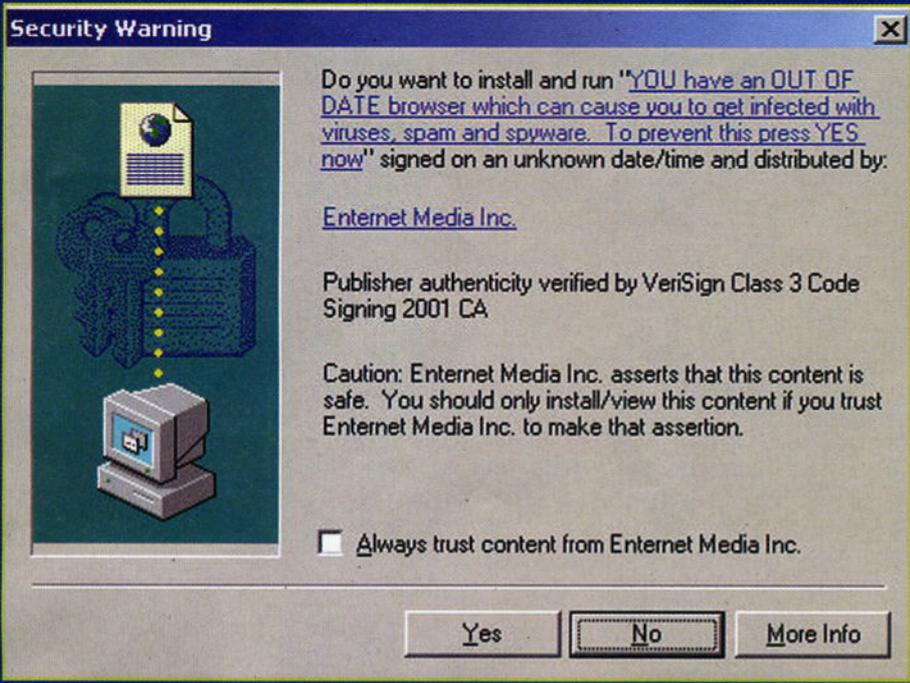
Sono molti i programmi shareware, cioè software con un periodo di prova gratuito o con funzioni limitate, che si possono scaricare e installare dalla rete. Alcuni di essi, però, installano automaticamente anche dei programmi spia che si occupano di redirezionare il nostro browser internet verso determinati siti web, oppure di raccogliere informazioni sul nostro conto e mandarle a terze parti per l'invio di pubblicità personalizzata, eccetera. Tra i programmi più a rischio segnaliamo Bonzi Buddy, Dope Wars, ErrorGuard, Grokster, Kazaa, Morpheus, RedLight, WeatherBug, EDonkey2000 e WildTangent.

Una cupola radar a Menwith Hill, un'installazione della R.A.F. con la capacità di captare le trasmissioni via satellite utilizzate da Echelon

:: Software-spia

Abbiamo già parlato in queste pagine dei cosiddetti spyware, programmi realizzati appositamente per spiare i nostri movimenti virtuali tramite il PC di casa. Gli spyware, però, non si limitano a spiarci, ma compiono anche delle azioni che possono essere estremamente dannose o fastidiose. Possono inviare i nostri dati senza autorizzazione ai programmatori, prendere parzialmente il controllo del nostro computer o di alcuni programmi, e altro ancora. Il termine, il cui significato attuale si deve a un rapporto del 2000 sulla sicurezza di Gregor Freund, fondatore di Zone Labs, indica una grande varietà di software con le funzioni più disparate. Secondo uno studio di due anni fa condotto da America On Line e dalla National Cyber-Security Alliance, il 61% dei computer analizzati aveva installata qualche forma di spyware e il 92% dei possessori di questi computer erano del tutto ignari della loro presenza. Il 91% di

KEYLOGGER

I programmi chiamati Keystroke Logger o più semplicemente Keylogger sono software realizzati per registrare tutti i pulsanti della tastiera che vengono premuti dalla persona che usa il PC infetto. Possono essere utilizzati in modo lecito per controllare eventuali errori di programmazione o di inserimento dati, oppure per tenere sotto controllo la produttività dei dipendenti di un'azienda... Ma possono anche essere usati in modo illecito per recuperare dati, come nomi e password utilizzati per accedere a programmi e siti internet, in modo da permetterne l'accesso anche all'autore del Keylogger. Molti anti-spyware sono in grado di identificare e bloccare queste applicazioni ed è inoltre consigliabile avere un firewall che controlli tutti i programmi in esecuzione, se non vogliamo farci rubare le password per il nostro account bancario online o altri dati estremamente importanti.

Le fondamenta di una torre di guardia vicina al sito "Antenna 1" nella ex-stazione di raccolta dati Echelon di Silvermine, vicino a Cape Peninsula, in Sudafrica

Un avviso che compare in una finestra del nostro browser internet ci informa che siamo infetti: non crediamogli, è un falso anti-spyware che vuole essere installato

essi affermò di non aver dato alcun permesso a terze parti di installare software sul proprio PC.
Secondo i dati statistici relativi ai rapporti inviati alle case di software che producono programmi anti-spyware, nove computer su dieci collegati alla rete sono infetti. Le varie versioni del sistema operativo Microsoft Windows sono in assoluto le più attaccate da questi 007 virtuali, e l'uso di Internet Explorer è per loro un'autentica manna dal cielo, poiché la sua stretta integrazione nel sistema operativo stesso fa sì che tali programmi abbiano accesso diretto a parti vitali del computer, potendo modificare codici di registro e funzionalità di vari programmi e applicazioni. Se possibile, quindi, è decisamente meglio utilizzare un altro browser internet (come, ad esempio, Mozilla Firefox) o addirittura un altro sistema operativo (come Linux o, nel caso di un computer Mac, MacOS).
Per liberarsi da queste infestazioni elettroniche è necessario installare un programma anti-spyware e mantenerlo costantemente aggiornato, facendo attenzione ai siti che si vanno a visitare in rete ed evitando accuratamente di cliccare su banner pubblicitari o di installare "barre" aggiuntive apparentemente innocue che, in realtà, possono metterci nei guai.
I creatori di spyware, però, non sono rimasti con le mani in mano e hanno prodotto una grande quantità di falsi prodotti anti-spyware che, una volta installati, non solo non tolgono le infestazioni presenti, ma ne aggiungono di proprie, autodifendendosi da eventuali altri attacchi. Se dovesse capitarvi di finire su qualche pagina internet dove una finestra a comparsa vi avvisa che è stato rilevato un virus o uno spyware, con scritte come "clicca qui per risolvere l'infezione", non fatelo! Normalmente, il collegamento porta all'installazione di uno di questi programmi anti-spyware finti. La lista si allunga ogni giorno, ma, a titolo di esempio, vi elenchiamo i nomi di alcuni di questi programmi molto pericolosi: errorsafe, Pest Trap, SpyAxe, AntiVirus Gold, SpywareStrike, Spyware Quake, WorldAntiSpy, Spylocked, SysProtect, Spy Sheriff, Spy Wiper, PAL Spyware Remover, PSGuard, MalWare, WinAntiVirus Pro 2006, WinFixer, Spydawn e ContraVirus.

ANTI-SPYWARE

I programmi sicuri che possono essere utilizzati per monitorare e cancellare spyware eventualmente presenti sul nostro sistema o tentativi di intrusione di vario tipo sono decisamente molti, e non resta che l'imbarazzo della scelta. Tra i più famosi, diffusi ed efficaci, ricordiamo: Ad-Aware, Bugoff, CA Anti-Spyware, CWShredder, Counterspy, Ewido Networks, HijackThis, Hitman Pro, NoAdware, Real-time Protection, RottkitRevealer, Spy Sweeper, SpyCatcher Express, SpyHunter, SpySubtract, Spybot – Search & Destroy, Spyware Doctor, Spyware Removal, System Safety Monitor, Windows Defender, Windows Malicious Software Removal Tool, XOFTspy Portable Anti-Spyware, Zerospyware e EAcceleration.

P2P A RAZZO

Modificando le impostazioni di Windows, i programmi per il File Sharing hanno la possibilità di contattare più velocemente le fonti e trovare prima quello che stiamo cercando.

Non importa quale programma P2P stiamo usando. Per avere le migliori prestazioni, dobbiamo assicurarci che abbia la massima libertà nel comunicare via Web. Per garantire un'impostazione ideale, possiamo eseguire alcune modifiche a Windows XP.

LIBERO DAI LIMITI

Ora che ce lo possiamo permettere, modifichiamo le impostazioni di uTorrent per consentirgli di lavorare al massimo delle sue possibilità. Facciamo clic sull'icona Impostazioni e selezioniamo la voce Avanzate. Cerchiamo nella finestra la voce net.max_halfopen, che normalmente è impostata su un valore di 8. Inseriamo un nuovo valore di poco inferiore al limite che abbiamo impostato con xp-AntiSpy.

:: Un problema di sicurezza

A partire dall'introduzione del Service Pack 2, le impostazioni predefinite di Windows XP integrano un sistema di controllo sui tentativi di connessione "incompleti" verso il Web. Si tratta di una misura di sicurezza che gli sviluppatori Microsoft hanno introdotto per ridurre l'attività di alcuni virus che, una volta installati su un PC, cercano di collegarsi ad altre macchine per diffondersi via Web.

La limitazione non li blocca, ma ne rallenta l'azione. In pratica, quando il sistema rileva che sono stati effettuati più di 10 tentativi di questo tipo, ne riduce la frequenza formando una coda che riduce la velocità di connessione.

:: Effetto collaterale

È difficile capire se l'accorgimento introdotto con il Service Pack 2 abbia contribuito davvero a ridurre la diffusione dei virus. Di certo, però, ha rallentato l'attività dei programmi di file sharing. Per scambiare

informazioni con gli altri PC collegati al circuito, infatti, tutti i software P2P eseguono tentativi di connessione molto simili a quelli usati dai virus.
Per evitare il blocco, tutte le versioni più recenti di eMule e Torrent hanno adottato un'impostazione predefinita che limita il numero di connessioni parziali a un numero inferiore di 10. In alcuni casi, però, l'accorgimento non è sufficiente e i programmi mostrano una certa instabilità.

:: Apriamo le porte

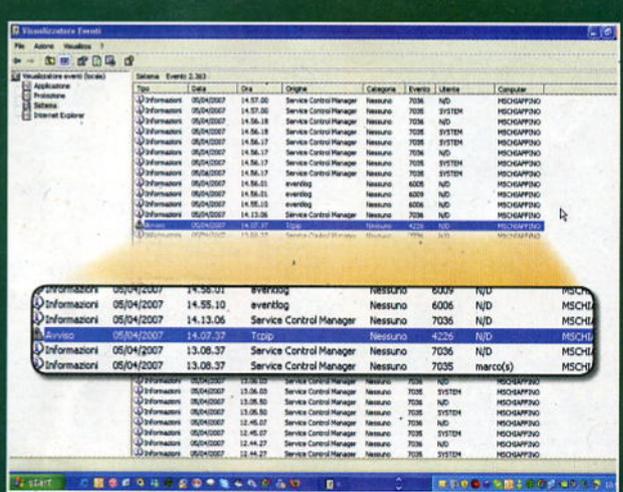
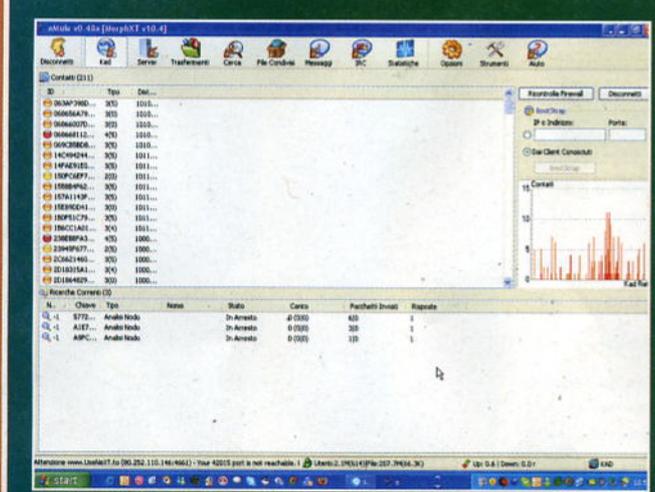
La modifica delle impostazioni può essere eseguita attraverso il registro di sistema, ma richiede alcuni interventi piuttosto delicati e la sostituzione di alcuni file di sistema. La via più pratica è quella di usare un programma che compia queste operazioni al posto nostro, come quello disponibile al sito Internet www.xp-antuspy.org.
Il programma, pensato per intervenire sulle impostazioni di Windows che normalmente non sono raggiungibili, prevede una funzione specifica che consente di aumentare il numero di connessioni simultanee e può consentirci di risolvere il problema una volta per tutte.

:: Anche con Vista

La limitazione al numero di connessioni parziali è presente anche nel nuovo sistema operativo di Microsoft. Anche in questo caso, su Internet si trovano alcuni programmi in grado di modificare le impostazioni del sistema. Considerata la giovane età di Vista, l'uso di qualsiasi programma "non ufficiale" che intervenga sul sistema operativo è da considerare troppo rischiosa e, quindi, sconsigliabile.
Limitiamoci quindi a verificare che, nelle impostazioni del nostro programma di File Sharing, le regolazioni prevedano un numero di tentativi simultanei di connessione "parziale" inferiore a dieci. ■

DIAMOGLI SPAZIO

Una volta modificate le impostazioni di Windows, possiamo intervenire sulle impostazioni di eMule per consentire al programma di sfruttare le nuove possibilità di connessione. Apriamo la sezione Opzioni Avanzate all'interno delle Opzioni e cerchiamo la voce N° Massimo Connessioni Parziali Aperte. Inseriamo un valore inferiore al limite massimo che abbiamo impostato nel sistema.

VERIFICHIAMO SE ESISTE IL PROBLEMA

1 Prova sul campo
Un piccolo esperimento ci permette di scoprire se l'uso del nostro programma preferito di File Sharing provoca il blocco delle connessioni parziali. Per prima cosa avviamo il programma che usiamo di solito, per esempio eMule, e colleghiamoci a un qualsiasi server. Lasciamo attivo il programma per qualche minuto.

2 Avviso nascosto
Apriamo il Pannello di controllo, selezioniamo Strumenti di amministrazione e facciamo doppio clic su Visualizzatore eventi. Controlliamo la voce Sistema: se nella colonna Evento c'è la voce 4226, Windows ha attivato la limitazione.

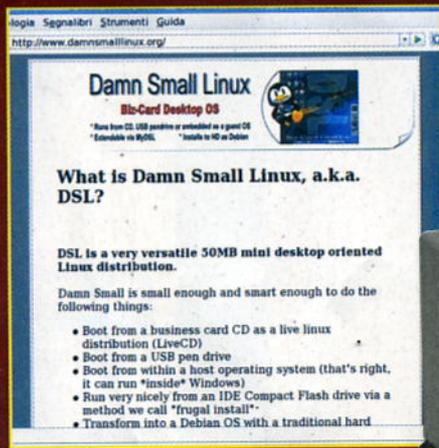
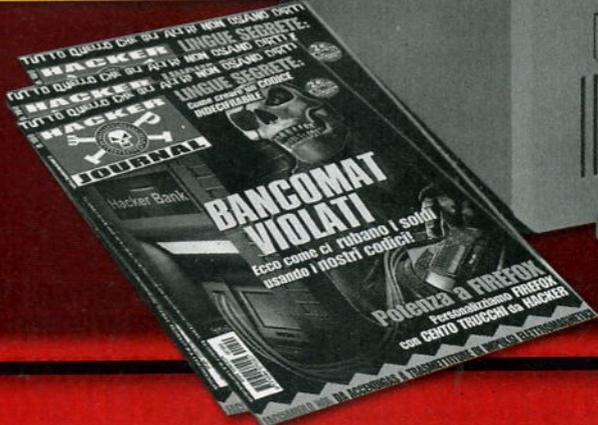
La fonte dell'ETERNA GIOVINEZZA

Scopriamo come ridare vita ad un computer con molti anni sulle spalle...

Nella nostra cantina, tra polvere e cianfrusaglie varie, abbiamo ritrovato un qualche reperto archeologico della prima era informatica, come un vecchio PC 586 d'annata o un velocissimo (per l'epoca, s'intende) Pentium II? Bene, è venuto il momento di togliere la polvere da questi preziosi cimeli e riportarli in vita. Per questo miracolo ci serviremo di una distribuzione Linux minimale: una lustratina all'hardware e con la nostra macchina d'altri tempi potremo navigare comodamente in Internet, scrivere documenti ed ascoltare la nostra musica preferita. Nella seconda parte dell'articolo, invece, vedremo come migliorare le prestazioni di un'installazione Linux preesistente, così da poter utilizzare distro recenti anche su PC "di vecchio pelo".

:: Un sistema davvero minimale

Di distribuzioni Linux ridotte ai minimi termini ne esistono a bizzeffe: Feather Linux, Puppy, Austrumi, per citarne solo alcune. Nel nostro caso si è optato per Damn Small Linux (DSL), che in 50MB di spazio fornisce un completo ambiente grafico con un vasto parco software, il tutto avendo come richieste minime di sistema una CPU 486DX e 16MB di ram; vediamo quindi come installare DSL sull'hard disk e come configurarla a puntino.

Dal sito della distro scarichiamo l'immagine ISO della nuova versione 4.0, quindi creiamo il CD di avvio dando in pasto il file ISO al nostro software di masterizzazione preferito: il file da prelevare sarà dsl-4.0.iso ma, nel caso in cui il CD generato da questa immagine non dovesse avviarsi correttamente sul nostro PC, proviamo a scaricare il file dsl-4.0-syslinux.iso (maggiormente compatibile con hardware vecchio).

Il sito di Damn Small Linux. Le caratteristiche di questa piccola distro sono invitanti...

:: Avviamo la distro dal CD

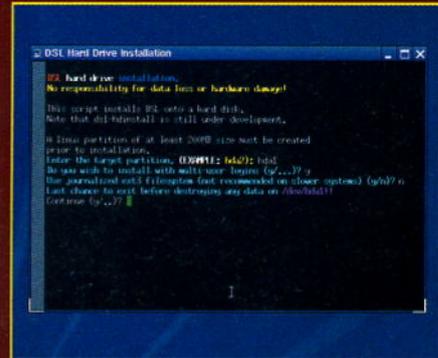
Al boot dal CD ci troveremo davanti alla schermata d'avvio: qui digitiamo sulla tastiera "dsl lang=it" e schiacciamo Invio. Dopo una manciata di secondi comparirà l'ambiente grafico: in basso troviamo l'abituale pannello, in alto a sinistra le icone per raggiungere le directory ed i programmi principali, in alto a destra invece abbiamo un utile monitor di sistema. A questo punto, presa confidenza con il desktop, possiamo procedere con l'installazione di DSL sul nostro disco rigido. Prima di fare ciò bisogna individuare la partizione da usare per l'operazione: nei vecchi PC l'hard disk principale ha come nomenclatura su Linux /dev/hda (a meno di un utilizzare dischi SCSI, in questo caso il dispositivo si chiamerà /dev/sda); quindi, la prima partizione sul primo disco rigido si chiamerà /dev/hda1, la seconda partizione sul secondo disco /dev/hdb2 e così via.

Il desktop di DSL: semplice, pratico e veloce. L'ideale per un vecchio PC!

Ora controlliamo quali sono le partizioni disponibili sull'hard disk. Apriamo una console di root: clickiamo sul primo pulsante "DSL" nel pannello in basso e, nel menu che appare selezioniamo XShells > Root Access > Transparent. Al prompt scriviamo "cfdisk /dev/hda": verranno visualizzate le partizioni sul disco, con le relative dimensioni. Nell'elenco rintracciamo la partizione più adatta per accogliere DSL (bastano 200MB di spazio).

Adesso possiamo procedere con l'installazione su hard disk. Clickiamo sempre sul pulsante "DSL" ed andiamo su Apps > Tools > Install to Hard Drive. Comparirà una piccola finestra. Al suo interno digitiamo il nome della partizione scelta per l'installazione, ad esempio "hda1". Quindi abilitiamo i login multiutente premendo "y"; se il nostro computer è particolarmente lento non abilitiamo l'uso del filesystem journaled (risposta "n" alla domanda successiva), infine confermiamo di voler continuare con l'installazione premendo "y".

A questo punto verranno copiati sull'hard disk i file della distribuzione. Fatto ciò, ci verrà chiesto se vogliamo installare il bootloader: rispondiamo di sì con "y".

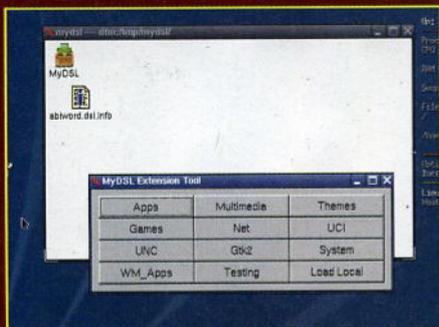
Alla domanda che segue scriviamo "g" per installare il boot loader Grub. Per finire, digitiamo "y" per riavviare la macchina.

I pochi passaggi necessari per installare DSL sull'hard disk.

:: Il vecchio PC è rinato

Al primo avvio di DSL da hard disk ci verrà chiesto di inserire le password per gli utenti root e dsl. Fatto questo, ritroveremo ad attenderci lo stesso desktop presente nella versione su CD della distro. Ora possiamo aggiungere del software a quelli installati per default: ad esempio, proviamo ad aggiungere al nostro sistema l'ottimo word processor Abiword; per fare questo clickiamo sull'icona MyDSL in alto a sinistra, quindi sull'icona MyDSL nella finestra che appare. A questo punto nella finestra "MyDSL Extension Tool" entriamo nella sezione "Apps" nell'elenco che compare clickiamo sulla voce "abiword.dsl", quindi premiamo il pulsante "Download". Terminati scaricamento ed installazione, potremo lanciare Abiword dal pulsante "DSL" in basso, entrando nel sottomenu "MyDSL".

:: Una Debian ridotta all'osso

Installare programmi con MyDSL è senz'altro comodo, ma con DSL è possibile fare di più: infatti, possiamo trasformare la nostra piccola distro in una Debian a tutti gli effetti! Il vantaggio principale sarà costituito da un parco software sterminato. Per 'debianizzare' il sistema, quindi, clickiamo sul pulsante "DSL" nel pannello, quindi andiamo su Tools > Enable Apt. Ora abbiamo a nostra disposizione i potenti strumenti di gestione dei pacchetti di Debian: per installare il web browser

testuale Lynx (un fulmine per navigare!), ad esempio, scriviamo in una console di root "apt-get install lynx".

Con MyDSL possiamo aggiungere facilmente nuovi programmi al sistema.

:: Trucchi per tutti i gusti

Ora qualche trucco che può essere utile per diminuire la ram occupata dal sistema, sia nel caso si utilizzino distribuzioni minimali come DSL, sia nel caso in cui il nostro PC arranchi nell'uso quotidiano delle distro 'normali'. Ci troviamo a nostro agio con il software fornito, ad esempio, con un'installazione di Ubuntu 7.10 ma il nostro povero PC con 256MB di ram, pur funzionando perfettamente, non ci consente un multitasking degno di questo nome? Iniziamo col cambiare ambiente grafico: Gnome e KDE richiedono quantità ingenti di ram per funzionare, XFCE è invece più parco nell'occupazione delle risorse, pur fornendo un desktop completo e ricco di funzionalità; ancora più leggeri sono i cosiddetti window manager, ambienti grafici essenziali ed estremamente funzionali: tra i tanti meritano una menzione icewm e fluxbox.

Con il window manager fluxbox il nostro vecchio PC volerà letteralmente...

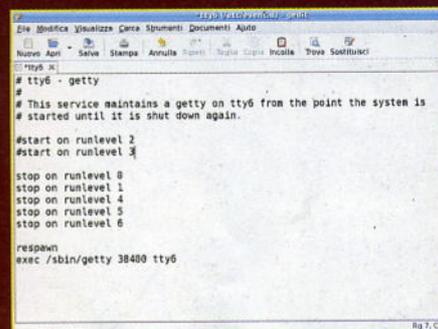
:: Quando la ram è agli sgoccioli

Il passo successivo è quello di ridurre il numero di servizi lanciati al boot della macchina. Gli strumenti per fare ciò variano da distribuzione a distribuzione, su Ubuntu è possibile utilizzare sysv-rc-conf; lanciamolo con "sudo sysv-rc-conf" in una console ed eliminiamo dal runlevel 2 (il runlevel multiuser di default) tutti i servizi che non ci servono: in Ubuntu 7.10, su di una comune macchina desktop possiamo togliere ad esempio apport, avahi-daemon (se non facciamo uso di questa implementazione di Zeroconf), bluetooth (se tale interfaccia non ci serve) e così via. Certo, ciò che otterremo sarà magari solo una manciati di MB liberi in più all'avvio ma, quando la ram è agli sgoccioli, anche interventi marginali possono giovare al buon funzionamento della macchina. Se la memoria scarseggia in modo preoccupante è possibile inoltre ridurre il numero di console virtuali disponibili (6 per default). Per fare questo basta intervenire nel file /etc/inittab e cancellare le righe relative alle console virtuali da eliminare; ad esempio, per togliere le console 5-6 commentiamo con '#' le righe seguenti:

```
5:2345:respawn:/sbin/getty tty5
6:2345:respawn:/sbin/getty tty6
```

facendole diventare così:

```
#5:2345:respawn:/sbin/getty tty5
#6:2345:respawn:/sbin/getty tty6
```

Se init è stato sostituito da upstart
Nelle ultime release di Ubuntu upstart ha preso il posto di init. Quindi, per ridurre il numero di console aperte dovremo agire in altro modo. Entriamo con un editor nel file /etc/default/console-setup ed individuiamo la linea 'ACTIVE_CONSOLES="/dev/tty[1-6]': modifichiamola indicando le console che vogliamo siano attive; ad esempio, per avere 3 console cambiamola in 'ACTIVE_CONSOLES="/dev/tty[1-3]"'.

Le righe da modificare in Ubuntu per togliere di mezzo qualche console virtuale.

Ora rintracciamo i file di configurazione delle console da noi disattivate (seguendo l'esempio, dalla 4 alla 6): si tratta dei file tty4, tty5 e tty6 presenti nella directory /etc/event.d. In ciascuno di questi file, quindi, rintracciamo le linee inizianti per start (ad esempio, "start on runlevel 2") e commentiamole inserendo il carattere '#' ad inizio riga.

LINK UTILI

http://www.damnsmalllinux.org/
http://featherlinux.berlios.de/
http://www.puppylinux.org/
http://www.xfce.org/
http://fluxbox.sourceforge.net/

Prima regola: PROTTEGGERSI!!!

Andiamo alla scoperta di due software di sicurezza dalle caratteristiche diverse ma ugualmente efficaci

La vita è di un internauta è una giungla e non ci sogneremmo mai di girare per la giungla indifesi ecco quindi due programmi che potrebbero coprirci le spalle durante i nostri viaggi, uno gratis e l'altro no ma si sa, alle volte la qualità bisogna pagarla...

:: ThreatFire AntiVirus Free Edition 3

Molti di noi hanno imparato a proprie spese che i sistemi di sicurezza su un computer non bastano mai. Mentre un tempo era sufficiente un semplice antivirus, oggi abbiamo bisogno di tutta una serie di applicazioni che, in teoria, fanno le stesse cose, ma che in pratica ci offrono tipi diversi di protezione. È proprio il caso di ThreatFire, un efficace antivirus che può agire da solo ma che è anche capace di "aiutare" l'antivirus che abbiamo già installato sul nostro computer per potenziarne l'efficacia. Questo software ci protegge da tutti i tipi di minacce, dai classici virus, ai trojan, dai rootkit agli spyware. L'interfaccia del programma è semplice. Sulla sinistra abbiamo i pulsanti delle funzioni principali e al centro la finestra di dialogo. Security Status ci tiene aggiornati in tempo reale sulla situazione del nostro sistema. Start Scan è lo strumento di analisi antivirus che ci permette di fare una scansione mirata o generale. Threat Control ci permette tra l'altro di visualizzare i file in quarantena o di consentire l'esecuzione di un determinato processo. Advanced Rules ci permette di personalizzare le regole di controllo e Settings è un utile strumento per programmare gli aggiornamenti del nostro antivirus. Un po' meno versatile della versione a pagamento, questo antivirus è poco avido di risorse e non rallenta il nostro computer. La semplicità e la leggerezza sono proprio le caratteristiche che fanno di ThreatFire un ottimo strumento di difesa che possiamo mantenere attivo anche se abbiamo già un altro antivirus.

:: System Surveillance Pro 4.8

Il rapido diffondersi di Internet in tutte le nostre case ha creato il problema del rapporto fra la Rete e i più piccoli. Fermo restando che la soluzione migliore resta sempre la presenza di un adulto, i vari pacchetti di sicurezza in commercio (ad esempio quelli di Norton e McAfee) e lo stesso Windows Vista offrono strumenti per il cosiddetto "controllo parentale". Si tratta di soluzioni che cercano di impedire la navigazione su siti inadatti ai bambini e ai minori in generale. Esistono tuttavia software espressamente dedicati a questo scopo, generalmente più efficaci. Uno dei più affidabili è System Surveillance Pro 4.8. Vero e proprio sistema di sorveglianza delle attività svolte su un computer, registra i programmi lanciati, i siti Web visitati, i messaggi istantanei inviati e, a intervalli regolari, memorizza le schermate del computer. Il programma è capace di spedire i rapporti via email e ha uno strumento per bloccare o rilevare la navigazione in siti di carattere pornografico. Inoltre è possibile usare parole chiave personalizzate per aumentare il livello di sicurezza e bloccare qualsiasi tipo di sito. Il programma è capace di lavorare in modo molto discreto, senza appesantire l'uso della macchina e senza che l'utente si accorga della sua presenza. Per aprire il pannello di controllo, è necessario passare per il menu Start e inserire una password, quindi solo l'amministratore può gestirne le funzioni. Non è possibile bloccarne il funzionamento nemmeno tramite il Task Manager di Windows. Purtroppo Golden Plains Software ci concede solo una settimana per provarlo, un tempo un po' troppo breve per apprezzarne a pieno l'efficacia e le notevoli potenzialità.

SCHEDA

ThreatFire AntiVirus Free Edition 3
Prezzo: Gratuito. La versione Pro costa 19,95 dollari
Editore: PC Tools
Sito: www.threatfire.com

QUATTORD. ANNO 6 - N°141 - 20 DICEMBRE 2007 / 9 GENNAIO 2008 - €2,00
WLF PUBLISHING